INSTITUTO DE ENSINO SUPERIOR - FACULDADE LABORO
TECNÓLOGO EM REDES DE COMPUTADORES

EDGERSON ZAIDAN TAVARES DE SOUSA
RAFAEL GLEYSON BEZERRA FERREIRA

BLOCKCHAIN: Conhecendo a ferramenta de registro de transações com criptomoedas.

TRABALHO DE CONCLUSÃO DE CURSO

SÃO LUÍS - MA
2019

EDGERSON ZAIDAN TAVARES DE SOUSA
RAFAEL GLEYSON BEZERRA FERREIRA

BLOCKCHAIN: Conhecendo a ferramenta de registro de transações com criptomoedas

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Esp. Carlos Rayllan Lima Sousa

SÃO LUÍS - MA
2019

EDGERSON ZAIDAN TAVARES DE SOUSA
RAFAEL GLEYSON BEZERRA FERREIRA

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: / /

BANCA EXAMINADORA

_____

Prof. Esp. Carlos Rayllan Lima Sousa (Orientador)

_____

Prof. Ms. Milson Louseiro Lima

_____

Prof. _____

Dedicamos este trabalho aos nossos pais, amigos, familiares e aqueles que sabem que só a luta muda a vida!

AGRADECIMENTOS

Primeiramente agradecemos a Deus, afinal sem Ele nada é possível, agradecemos a nossa família pelo apoio e compreensão, aos nossos amigos que nos ajudaram de forma direta ou indireta.

Também somos gratos a Faculdade Laboro que sempre prezou pela qualidade no ensino ofertado.

Agradecemos aos nossos estimados professores, coordenador e orientador, foram peças fundamentais para esta parte da trilha do conhecimento.

Fica aqui o nosso agradecimento a todos aqueles que contribuíram, contribuem e contribuirão para o nosso desenvolvimento acadêmico e social.

RESUMO

SOUSA, Edgerson Zaidan Tavares de; FERREIRA, Rafael Gleyson Bezerra. **BLOCKCHAIN:** Conhecendo a ferramenta de registro de transações com criptomoedas. 2019. 29 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

Apresentado em 2009 por um programador com o codinome Satohi Nakamoto surgiu o Bitcoin, moeda virtual que não depende de um banco ou um órgão centralizado, uma moeda virtual que não pertence a nenhuma entidade ou país, junto com o Bitcoin surgiu o Blockchain a ferramenta que registra as transações realizadas com criptomoedas, mas com o surgimento das criptomoedas e das ferramentas de registro também surgiram dúvidas acerca de sua confiabilidade. Este trabalho traz a apresentação da moeda virtual e da ferramenta que registra as transações, o método de operação e as ferramentas que são usadas. A função hash traz segurança adicionando ao bloco de transação uma chave imutável, procedimento esse que traz segurança nas operações com criptomoedas. Aliada a uma rede p2p, descentralizada que fornece as informações para todos os nós conectados à rede, tornando-a transparente e confiável eliminando a necessidade de um agente regulador o que geraria custos para a realização das transações.

Palavras-chave: Bitcoin. Blockchain. Criptografia. Função-hash. Descentralização.

ABSTRACT

SOUSA, Edgerson Zaidan Tavares de; FERREIRA, Rafael Gleyson Bezerra. **BLOCKCHAIN:** Knowing the transaction registration tool with cryptocurrencies**.** 2019. 29 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

Presented in 2009 by a programmer with the codename Satohi Nakamoto emerged the Bitcoin, virtual currency that does not depend on a bank or a centralized organ, a virtual currency that does not belong to any entity or country, along with Bitcoin emerged the Blockchain the tool that records transactions performed with Cryptocurrencies, but with the emergence of cryptocurrencies and registration tools also arose doubts about their reliability. This paper brings the presentation of the virtual currency and the tool that registers the transactions, the method of operation and the tools that are used. The hash function brings security by adding to the transaction block an immutable key, this procedure that brings security to operations with cryptocurrencies. Allied to a P2P, decentralized network that provides the information for all nodes connected to the network, making it transparent and reliable eliminating the need for a regulatory agent which would generate costs for the realization of transactions.

Keywords: Bitcoin. Blockchain. Encryption. Function-Hash. Decentralization.

LISTA DE FIGURAS E ILUSTRAÇÕES

Figura 1 – Entradas e saídas da função hash 18
Figura 2 – Função hash sofrendo colisão 19
Figura 3 – Função hash revertida..... 19
Figura 4 – Demonstração da função hash em texto plano 20
Figura 5 – Hash gerado..... 20
Figura 6 – Campos de transação 21
Figura 7 – Registros encadeados..... 21
Figura 8 – Dados de um registro 22
Figura 9 – Processo de validação do registro 23
Figura 10 – Arquitetura cliente-servidor 23
Figura 11 – Arquitetura p2p..... 24
Figura 12 – Rede Maior Cadeia 26

SUMÁRIO

1 INTRODUÇÃO 10

2 BITCOIN E BLOCKCHAIN 12

2.1 Bitcoin..... 12

2.1.1 Benefícios do Bitcoin..... 13

2.1.2 Potencial contra a pobreza e a opressão 15

2.2 Blockchain..... 15

2.2.1 Blockchains públicos e privados..... 17

3 COMPONENTES BLOCKCHAIN 17

3.1. Função hash..... 17

3.2 Transações em Blockchain 20

3.3 Redes p2p (peer-to-peer)..... 23

3.4 Mineração ou validação dos blocos 24

3.5 Ataque 51%..... 26

4 CONSIDERAÇÕES FINAIS 28

4.1 Trabalhos Futuros 28

REFERÊNCIAS..... 29

1 INTRODUÇÃO

Antes do surgimento das moedas, as transações eram realizadas através de trocas de alimentos, mantimentos, vestimentas e animais, onde as duas partes se davam por satisfeitas com a troca. As primeiras moedas surgiram no Reino da Lídia, território hoje denominado por Turquia, no continente europeu, os lídios começaram a usar diferentes metais, de diferentes pesos para realizarem trocas, criando assim as primeiras moedas, anos mais tarde surgiram as primeiras moedas cunhadas, processo no qual as moedas são gravadas com imagens ou nomes, criando assim um sistema monetário que se propagou por todo o mundo.

Atualmente cada país possui sua moeda, que é movimentada no país ou conjunto de países, movimentando a economia, tendo um valor muito forte tornando-a valorizada ou um valor de mercado mais baixo, o que a torna uma moeda fraca perante outros sistemas monetários espalhados pelo mundo. Esta evolução também se deu pelas revoluções industriais e sociais, o homem desde sempre está em meio as máquinas, e também está passando pela revolução tecnológica, onde vemos e vivemos uma constante mudança, onde as tecnologias mudam de forma muito rápida, gerando novos empregos, novos ramos, novas vagas ou extinguindo ocupações, empregos e cargos, e no meio de toda essa evolução as moedas continuam evoluindo, e surgiram as moedas virtuais e entre elas a mais conhecida, o Bitcoin.

O surgimento das criptomoedas, trouxe a necessidade de um método que faça o registro das transações. O Blockchain surgiu com a finalidade de fazer tal registro, fazendo-o de forma rápida, simples e segura, no decorrer deste trabalho temos a missão de aprofundar os conhecimentos a cerca desta nova ferramenta que tem modernizado e trazido mais segurança nas transações com criptomoedas e que também pode ser aplicado futuramente a outras aplicações das quais usamos e necessitam de uma modernização para acompanhar a evolução que a sociedade vive nos dias de hoje.

A necessidade conhecer e aprofundar o estudo acerca da ferramenta que contém os registros de transações feitas com criptomoedas levanta a seguinte questão: “Posso confiar num sistema que elimina o intermediador para fazer minhas transações?” A falta de conhecimento, divulgação e trabalhos que mostrem a funcionalidade, os objetivos e o funcionamento da ferramenta alimentam dúvidas semelhantes a dúvida citada acima. A solução para amezinhar, ou até mesmo sanar

todas as dúvidas relacionadas ao Blockchain é apresentar a sua origem, através de pesquisas e estudos, o seu funcionamento e os elementos que provam a segurança e qualidade da ferramenta utilizada para o registro das transações com criptomoedas, das quais temos como principal e mais conhecida o Bitcoin.

A concepção deste trabalho tem como objetivo a contribuição para o meio acadêmico e social apresentando de forma simples e objetiva o funcionamento do Blockchain, a ferramenta que registra as transações com criptomoedas, das quais temos como principal e mais conhecida o Bitcoin que tem se difundido ao longo dos anos e ganhado adeptos que fazem uso constante desta moeda que não possui nacionalidade. A apresentação dos elementos que constituem e fazem a ferramenta funcionar é importante para o conhecimento daqueles que fazem uso da mesma e não possuem informações mais concretas e relevantes sobre o sistema. De forma simplificada podemos dizer que o objetivo deste trabalho é trazer uma “biografia” da ferramenta.

O objetivo de detalhar a ferramenta de forma simples e prática possibilitará o entendimento do leitor e trará mais credibilidade ao conteúdo apresentado, pois ao detalhar a ferramenta que organiza como um livro-caixa as transações de criptomoedas o leitor passa a entender o processo que traz segurança nas transações que ele realiza.

A principal metodologia adotada para a produção deste trabalho foi a análise de artigos, livros e trabalhos relacionados ao tema proposto, tal medida foi adotada para que o trabalho tenha uma fonte concreta, e credibilidade no conteúdo apresentado. O estudo e comparação com diferentes autores e seus posicionamentos foi de extrema importância, pois tal comparação nos permitiu ter um embasamento mais profundo que contribuiu bastante para a construção do trabalho.

A pesquisa bibliográfica e o pensamento crítico foram regras na idealização deste trabalho, tais práticas, além de proporcionarem a adição de conhecimento, nos deram a base e a credibilidade necessária para a construção deste trabalho.

2. BITCOIN E BLOCKCHAIN

2.1 Bitcoin

O Bitcoin surgiu em 2008, criado por um programador conhecido apenas pelo codinome Satoshi Nakamoto, de forma simples dizemos que o bitcoin é uma forma de dinheiro assim como o dólar, o real, o euro, ou o peso, a sua principal diferença é que ele é virtual, ou seja, não é palpável como moedas e cédulas como conhecemos hoje, logo o mesmo não pode ser emitido por nenhuma organização ou governo.

O bitcoin “caiu nas graças” de seus usuários por ser ideal para transações online, afinal o procedimento é rápido e seguro, outro ponto positivo dado ao bitcoin é o fato de seu valor de mercado ser determinado livremente pelos indivíduos que fazem uso da moeda. Acredita-se que a necessidade da exclusão de um terceiro intermediário de confiança nas transações online tenha sido o fator principal para a criação da moeda virtual.

> “Em definitivo, o Bitcoin é a maior inovação tecnológica desde a internet, é revolucionário, sem precedentes e tem o potencial de mudar o mundo de uma forma jamais vista. À moeda, ele é o futuro. Ao avanço da liberdade individual, é uma esperança e uma grata novidade.” (ULRICH, 2014, p. 16)

Para tornar mais claro o entendimento do Bitcoin, exemplificaremos como uma transação online era realizada antes do bitcoin:

Se Francisco necessitasse realizar o envio de R$ 500,00 para Antônia através da internet ele teria que depender de um serviço terceiro para realizar o envio como o *Paypal* ou Banco do Brasil. Estes terceiros possuem um registro do quanto os clientes possuem de saldo em conta. Quando Francisco envia R$ 500,00 para Antônia, é debitado o valor da conta de Francisco e creditado na conta de Antônia, se não houvesse o agente intermediário o mesmo dinheiro poderia ser gasto mais de uma vez, gerando assim o problema do gasto-duplo.

Até o surgimento do Bitcoin as transações online só poderiam ser realizadas desta forma para que não ocorresse o problema do gasto-duplo que geraria custos elevadíssimos caso não houvesse o agente intermediador.

Uma das verdades mais marcantes acerca do Bitcoin é fato de ele não ser apenas uma moeda livre de governos ou entidades, mas também o fato de ser um sistema global de pagamentos online e descentralizado. Além de tudo não é escasso, e não pode gear danos ao meio ambiente, como o uso de papel ou metais para a sua confecção, pois trata-se de uma moeda 100% digital.

Ulrich (2014, p. 17) afirma que “a invenção do Bitcoin é revolucionária e resolve o problema do gasto-duplo sem que haja a necessidade de um terceiro.” O blockchain faz isso distribuindo o registro a todos os usuários através de uma rede *peer-to-peer,* na tradução literal, ponto-a-ponto.

A existência de ambos, Bitcoin e Blockchain está ligada de forma muito forte. Segundo Ulrich (2014) “O Bitcoin é uma moeda de código aberto que não depende de uma autoridade central”. Já Swan (2015) define o bitcoin como “uma moeda digital independente que utiliza técnicas de criptografia para realizar transferências e pagamentos”.

As transações que são realizadas com bitcoin são registradas em um “livro-razão” denominado *blockchain*, este registro é público e distribuído, ou seja, todos tem acesso, em palavras mais simples o blockchain é de forma simplificada um grande banco de dados que contém todas as transações realizadas. Na seção Blockchain aprofundaremos o conhecimento para o entendimento da ferramenta e seus auxiliares.

> “Nasce uma nova tecnologia, voltada a economia e preocupada em fornecer uma alternativa a questões antes imaginadas por poucos. A importância recente refere-se ao fato dos governos poderem ditar os preços e custos de forma arbitrária sem levar em conta os avanços da área e não precisar seguir os preços de mercado.” (ARAÚJO; SILVA, 2017 p. 30)

Uma grande maioria das pessoas ainda resiste ao uso do Bitcoin e tem como principal questionamento o fato do Bitcoin não ser palpável e por isso não conseguem confiar na moeda virtual. Ulrich em seu livro “Bitcoin – A moeda na era digital” nos dá uma resposta clara acerca da resistência que muitos ainda tem em usar o Bitcoin, ele diz:

> “Ainda é uma moeda nova e flutuante que não é aceita por muitos comerciantes, tornando seus usos quase experimentais. Para entender melhor o Bitcoin, ajuda se pensarmos que ele não é necessariamente um substituto às moedas tradicionais, mas sim um novo sistema de pagamentos.” (ULRICH, 2014, p. 23)

2.1.1 Benefícios do Bitcoin

São muitos os benefícios atribuídos ao Bitcoin, mas o benefício que mais chama atenção é o de ele não depender de um agente intermediário de confiança e, como consequência disso as transações são mais rápidas e baratas se comparado com as transações feitas no modo tradicional pelas redes de pagamentos.

Mas por que as transações com Bitcoin são mais baratas? O que há de especial no Bitcoin? Ulrich (2014, p. 23) diz que “o Bitcoin faz com que micropagamentos e suas inovações sejam possíveis”, além disso ele afirma que o Bitcoin “é uma grande promessa de uma forma de reduzir custos de transação aos pequenos comerciantes”, como veremos mais a frente.

“Aliviar a pobreza global pelo facilitado acesso ao capital, proteger indivíduos contra controles de capitais e censura, garantir privacidade financeira a grupos oprimidos e estimular a inovação.” (ULRICH, 2014 p. 23) Este trecho mostra a esperança carregada não só por Ulrich, mas carregada também por grande parte

daqueles que fazem uso do Bitcoin e daqueles que sempre buscam uma sociedade com menos custos e mais qualidade.

> “Em primeiro lugar, Bitcoin é atrativo a pequenas empresas de margens apertadas que procuram formas de reduzir seus custos de transação na condução de seus negócios. Cartões de crédito expandiram de forma considerável a facilidade de transacionar, mas seu uso vem acompanhado de pesados custos aos comerciantes.” (ULRICH, 2014, p. 23)

Os comerciantes que desejam implementar pagamento através de cartão de crédito ou débito devem fazer a contratação de uma conta junto as empresas que administram os cartões, dependendo do contrato realizado entre as partes os comerciantes devem pagar as mais variadas taxas, taxas de administração, taxas de transação, taxas de extratos, taxas de manutenção entre outras que na maioria das vezes nem são importantes, a quantidade de taxas não é benéfico para o comerciante pois as mesmas se acumulam e consequente terão um alto valor no futuro, mas se o comerciante opta por não usar a “maquineta” de pagamentos com cartão ele corre o risco de ver suas vendas caírem drasticamente, afinal ele estaria indo na contramão da evolução dos pagamentos. Diante disso o comerciante fica num beco sem saída e na maioria das vezes acaba optando por aceitar as altas taxas impostas pelos sistemas administradores dos cartões.

> “Como Bitcoin facilita transações diretas sem um terceiro, ele remove cobranças custosas que acompanham as transações com cartões de crédito. O Founders Fund, um fundo de *venture capital* encabeçado por Peter Thiel, do PayPal e Facebook, recentemente investiu 3 milhões de dólares na companhia de processamento de pagamentos BitPay, por causa da habilidade do serviço em reduzir os custos no comércio online internacional.” (ULRICH, 2014, p. 24)

Os benefícios já atraem mais comerciantes, Ulrich (2014 p. 24) em seu livro diz que “pequenos negócios já começaram a aceitar bitcoins como uma forma de evitar os custos de operar com empresas de cartões de crédito.” Mas muitos não aceitam começaram a usar o Bitcoin apenas para evitar os altos custos com as empresas, outros comerciantes já aceitam e usam o Bitcoin devido a sua eficiência e velocidade que facilitam a transação, espera-se que mais comerciantes e pessoas adotem o Bitcoin, essa adoção será muito benéfica e fará com que o Bitcoin continue reduzindo os custos das transações.

Ulrich (2014) em seu livro fala que consumidores gostam dos estornos, no entanto, porque o sistema os protege de erros de comerciantes, inescrupulosos ou não. Isso mostra como as fraudes podem acontecer e por sua vez prejudicar uma ou ambas as partes. Consumidores podem também gozar dos outros benefícios que os cartões de crédito oferecem. E muitos consumidores e comerciantes provavelmente preferiram ater-se aos serviços tradicionais de cartões de crédito, mesmo com a disponibilidade dos pagamentos pela rede Bitcoin. Ainda assim, a ampliação do leque de escolhas de opções de pagamento beneficiaria a todos os gostos.

Ulrich (2014 p. 24) destaca uma das grandes promessas do bitcoin ao afirmar que “Com um acessível sistema de transferência de fundos, Bitcoin também é uma grande promessa ao futuro das remessas de dinheiro de baixo custo.” Tal afirmação anima aos usuários da moeda virtual e dá esperança por custos mais baixos.

2.1.2 Potencial contra a pobreza e a opressão.

Países subdesenvolvidos ou em estado de grave pobreza ou em países com sistemas autoritários de governo também podem se beneficiar do Bitcoin, afinal ele tem a capacidade e o potencial de ajudar pessoas que que vivem nessas condições, Ulrich (2014 p. 25) afirma que o Bitcoin tem o

> “potencial de melhorar a qualidade de vida dos mais pobres no mundo. Aumentar o acesso a serviços financeiros básicos é uma técnica antipobreza promissora, de acordo com estimativas, 64% das pessoas vivendo em países em desenvolvimento têm parco acesso a esses serviços, talvez porque seja bastante custoso a instituições financeiras tradicionais servir às áreas pobres e rurais.” (ULRICH, 2014, p. 25)

Muitos serviços bancários não chegam aos locais mais pobres devidos as dificuldades de desenvolvimento estrutural e social, e, diante dessas dificuldades muitos acabam migrando para serviços bancários que são oferecidos via celular para driblar os problemas enfrentados pela falta de serviços bancários locais.

“Serviços bancários por celular em países em desenvolvimento podem ser ampliados pela adoção do Bitcoin. Como um sistema aberto de pagamentos, o Bitcoin pode fornecer às pessoas nesses locais acesso barato a serviços financeiros, em uma escala global.” (ULRICH, 2014 p. 26)

2.2 Blockchain

Antes de falar sobre detalhes e princípios de funcionamento da Blockchain; precisamos saber sobre a gênese da tecnologia em questão. Em 1991 pesquisadores falaram sobre a tecnologia pela primeira vez, uma estrutura conceitual foi apresentada com uma ideia inicial destinada a documentos digitais com data e hora registradas, de modo que, posteriormente não seria possível data-los novamente. No entanto, o projeto não obteve ascensão, até que novamente foi mencionada por Satoshi Nakamoto em seu *paper “Bitcoin: A Peer-to-Peer Electronic Cash System”* (“Bitcoin: um sistema de dinheiro eletrônico peer-to-peer”.)

Segundo explicação de Lucena e Henriques (2016) “O blockchain surgiu com a criptomoeda Bitcoin e tem por objetivo ser um livro-razão em que todas as transações financeiras de todos os usuários de Bitcoin ficassem armazenadas de forma a não ocorrer problema de gasto duplo [...]”. No trecho citado é notável que os autores reafirmam a relação que há entre o Bitcoin e a tecnologia empregada no blockchain, tecnologia essa que é responsável por toda a segurança e armazenamento das transações da criptomoeda, partindo de outro ponto de vista podemos definir a tecnologia como um banco de dados descentralizado.

O blockchain é uma ferramenta que tem como objetivo a descentralização como medida de segurança. Um índice global é criado e tem como base os registros que são distribuídos e compartilhados de forma geral mostrando todas as transações que ocorrem dentro de uma determinada rede.

Acredita-se que é a primeira vez que o criador de uma tecnologia tão inovadora se encontra no total anonimato, existindo apenas especulações sobre acerca de sua identidade. Satoshi Nakamoto criador do Bitcoin e propulsor da Blockchain teve seu pontapé inicial nos trabalhos de ambas as tecnologias em 2009 quando o primeiro bitcoin foi minerado pelo mesmo, utilizando as tecnologias das quais ele aperfeiçoou. Anos se passaram e o Bitcoin tornou-se popular e a tecnologia subjacente veio a tornar-se ainda mais popular. Assim, a confusão e falta de clareza entre as pessoas partem desde da própria origem. Um produto e suas terminologias relacionadas se tornaram virais antes da tecnologia por trás dele. E quando a blockchain exibia seu potencial real, as pessoas tentavam relaciona-las com as terminologias bitcoin, o resultado foi total equívoco e confusão.

O uso da Blockchain permitiu que o Bitcoin fosse implementado de forma distribuída, de modo que nenhum usuário controlasse o dinheiro eletrônico e não existisse nenhum ponto de falha, dessa forma, promovendo e popularizando seu uso. Como seu principal benefício, existe a permissão de transações diretas entre usuários sem a necessidade de um terceiro intermediador confiável. Usando um mecanismo de autopoliciamento baseado no consenso com todos os nós da rede conectada, garantiu-se que apenas transações e blocos validos fossem adicionados à Blockchain. Sem estes intermediários a confiança necessária dentro de uma rede blockchain é legitima com o uso de quatro características chaves.

As principais características da Blockchain:

- Imutável – A blockchain faz um registro que não pode ser modificado depois que um bloco é adicionado, de forma alguma o mesmo poderá ser alterado. Criando-se confiança no registro da transação.

- Verificação de confiança – Independentemente, cada bloco é verificado por meio de modelos de consenso, fornecendo regras para validar o bloco que geralmente necessitará de um recurso escasso (poder de computação) demonstrando que foi feito um esforço adequado. Processo este, podendo ser exemplificado no bitcoins em sua mineração.

- Transparência – Por tratar-se de um arquivo aberto, qualquer parte poderá acessa-lo e auditar transações publicamente. A criptografia utilizada não necessariamente precisará identificar os usuários, porém, o vínculo de identidades é possível se necessário. Ajudando a assegurar a legitimidade dos usuários que estiverem praticando as transações.

- Descentralização – Sem nenhuma rede governamental ou órgão central, a blockchain mantém todos os usuários do nó conectados e em posição direta provendo um serviço cliente-servidor que garante maior confiabilidade por não tratar-se de um sistema centralizado.

2.2.1 Blockchains públicos e privados

"As redes blockchain podem ser categorizadas em dois grupos: blockchain pública ou "*permissionless*" (sem permissão, de acesso aberto), e blockchain federada/privada ou "*permissioned"* (com permissão e acesso controlado)." (GREVE et al.,2018)

Para que anonimamente pessoas criem contas e participem das redes blockchain existem as chamadas "Blockchains públicas". Oferecendo um nível de segurança entre partes sem existir nenhum conhecimento das partes relacionadas; essa confiança poderá permitir que os indivíduos e organizações façam transações diretamente, podendo dessa forma resultar em operações mais rápidas e com custos mais baixos.

O controle de acesso mais rígido, onde alguma confiança poderá estar presente entre os usuários são recursos encontrados na rede de "Blockchain privada". O conteúdo somente será acessível às partes permitidas. Nestes devidos sistemas todos trabalham para alcançarem juntos um processo com desincentivo para cometerem fraudes, ou caso contrário, o comportamento será reconhecido pelas organizações presentes.

3 COMPONENTES BLOCKCHAIN

Apesar de parecer complexa, a tecnologia blockchain pode ser simplificada se for examinada e detalhado cada aspecto de seus componentes, que por sua vez utilizam mecanismos já presentes na ciência da computação conhecidos e primitivos sistemas de criptografia, como por exemplo: Funções Hash criptográficas, assinaturas digitais, criptografia de chave assimétrica, entre outras.

3.1 Função *hash*

Um dos principais recursos usados na tecnologia blockchain é o *Hash* e sua execução conhecida como *hashing* é um método de aplicar aos dados a função *hash*, calculando uma saída única e relevante para qualquer que seja o tamanho de sua entrada (um texto, imagem ou arquivo). Permitindo que os indivíduos tomem os dados de entrada de forma independente e posteriormente compartilhem destes dados e obtenham o mesmo resultado, dessa forma, provando que em nenhum momento de toda a transição o arquivo teve seus dados alterados. A mais sutil alteração em qualquer um dos dados acarretará em uma saída totalmente divergente.

A função hash, nada mais é do que uma função matemática com propriedades bem especificas que são elas:

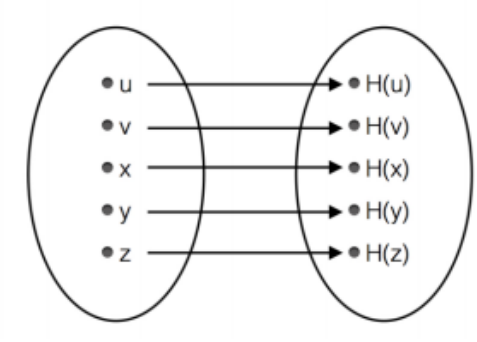
- Entradas podem ter sequencias de caracteres com qualquer tamanho;

- Uma sequência de caracteres de tamanho fixo será criada na saída;

- A função executará em um determinado tempo a entrada de n caracteres que deverá ser O(n)

Na figura 1, (u,v,x,y,z) demonstram entradas de quaisquer tamanhos para a função hash H(i). O tamanho que se aplicará na saída desta mesma função é fixo.

Figura 1: Entradas e saídas da função hash



Fonte: Narayanan et al, 2016, *adaptado*

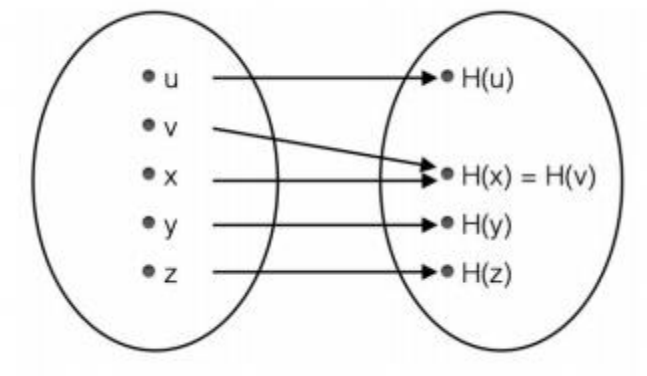
> "As propriedades acima definem uma função hash de maneira geral, suficientes para construir uma tabela de hash. No entanto, há mais duas propriedades normalmente desejadas em uma função hash, ou propriedades que caracterizam uma função hash criptográfico." (Narayanan *et al*, 2016):

- Resistente a colisões;

- Anti-reversão;

Quando duas ou mais entradas diferentes produzem na saída o mesmo hash, chamamos de colisão, como mostrado na figura 2:

Figura 2: Função hash sofrendo colisão



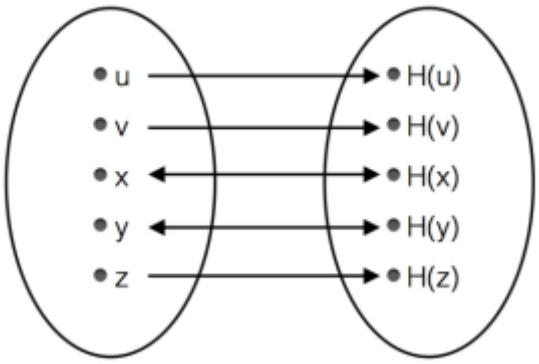
Fonte: Narayanan *et al*, 2016, *adaptado*

O termo “Resistente a colisões” significa que existe uma probabilidade mínima de que duas entradas produzam o mesmo hash. Não se pode afirmar a impossibilidade da ocorrência de colisões, uma vez que esta função possui um domínio caracterizado pela composição de todas as sequencias de caracteres possíveis. Apesar disso, funções de hash bem elaboradas possuem baixíssima probabilidade de colisão.

“A resistência a colisão permite a utilização do hash como síntese de mensagem. Por exemplo, para verificar se um arquivo baixado de um servidor na nuvem corresponde ao arquivo desejado, basta fazer a comparação de seus *hashes* ao invés de comparar todo o arquivo.” (Narayanan et al, 2016).

> “Ser anti-reversão significa que não é possível obter a mensagem de entrada x a partir do hash h(x). Esta característica é alcançada fazendo com que a probabilidade dos hashes na saída da função obedeçam a uma distribuição uniforme. Na prática, isto significa que não é possível correlacionar caracteres na entrada e na saída da função apenas observando a frequência com que eles aparecem.” (Narayanan et al, 2016).

Figura 3: Função hash revertida



Fonte: Narayanan *et al*, 2016, *adaptado*

A função SHA-256 projetada pela Agencia Nacional de Segurança dos EUA (NSA) é a principal função a ser utilizada pela Blockchain. Produzindo um *hash* com tamanho fixo de 256 bits. Facilitando o cálculo, o SHA-256 possui uma saída de 32 bytes (1 byte = 8 bits, 32 = 256 bits), geralmente sendo formado de hexadecimais de 64 caracteres.

As figuras 4 e 5 demonstram exemplos simples disso.

Figura 4: Demonstração da função hash em texto plano

Fonte: BLOCKCHAIN..., 2019

Na caixa de texto para exemplo foi utilizada a palavra “Pesquisa.” Com um ponto “.” no final, gerando um hash hexadecimal de 64bits especifico para aquela palavra.

Figura 5: Hash gerado

Fonte: BLOCKCHAIN..., 2019

Já nesta caixa de texto é utilizada a palavra “Pesquisa” sem a utilização do ponto no final, gerando novamente um hash hexadecimal de 64bits especifico para aqueles caracteres.

3.2 Transações em Blockchain (Registros)

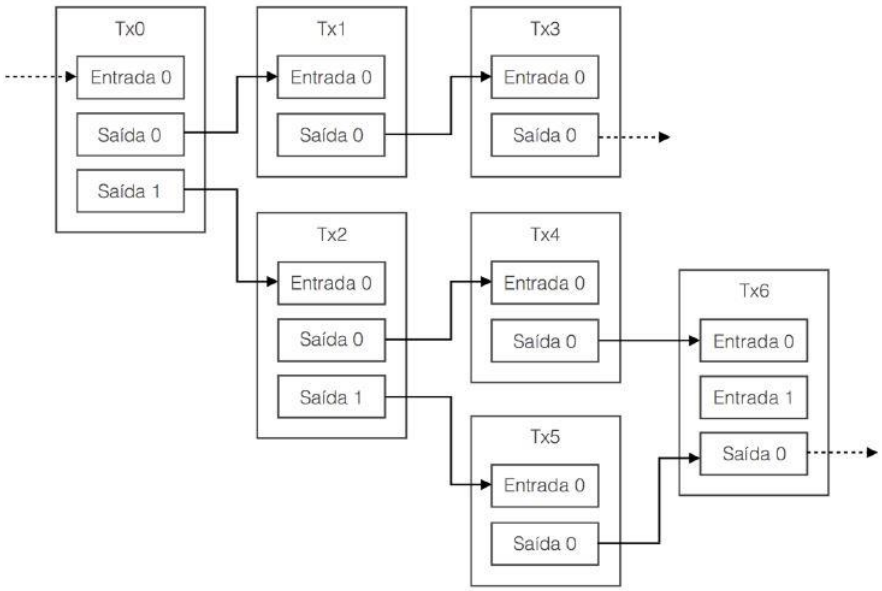
Assim como os blocos estão encadeados na tecnologia Blockchain, as transações também estão. Abaixo, a figura 1 mostra os campos que compõem um registro, também conhecido por transação, e a figura 2 faz ilustração do encadeamento dos registros encadeados através de suas entradas e saídas.

Figura 6: Campos de transação

Campo	Descrição
Metadados	Informações da transação como Id e tamanho.
Entradas	Vetor com informações de cada entrada da transação
Saídas	Vetor com informações de cada saída da transação

Fonte: PIRES 2016 p. 27

Figura 7: Registros encadeados



Fonte: PIRES 2016 p. 27

“O campo Metadados reúne informações gerais da transação como o tamanho da transação em bytes, quantidade de entradas e saídas, versão do protocolo e o id da transação, obtido a partir do cálculo de seu hash SHA256.” (PIRES, 2016 p. 28)

“O campo Entradas apresenta uma lista numerada de entradas desta transação. Cada entrada de uma transação deve fazer referência a saída de outra. Logo, neste campo há uma lista de id‘s de outros registros e o respectivo número da saída.” (PIRES, 2016 p. 28)

> “Estas saídas devem ser computadas como entradas nesta transação. Ainda no campo entrada são adicionadas uma assinatura digital e uma chave pública responsáveis por confirmar que aquela transação está autorizada a utilizar as saídas indicadas no campo Entradas.” (PIRES, 2016 p. 28)

No campo de saída é apresentado uma lista das saídas que devem ser utilizadas de forma numerada que futuramente serão utilizadas como entradas para transações futuras. Pires (2016 p. 28) diz que “este campo apresenta ainda um *hash* de chave pública que possui informações que condicionam a utilização dessas saídas

por outra transação.” Na próxima imagem temos uma ideia das entradas e saídas de um registro.

Figura 8: Dados de um registro

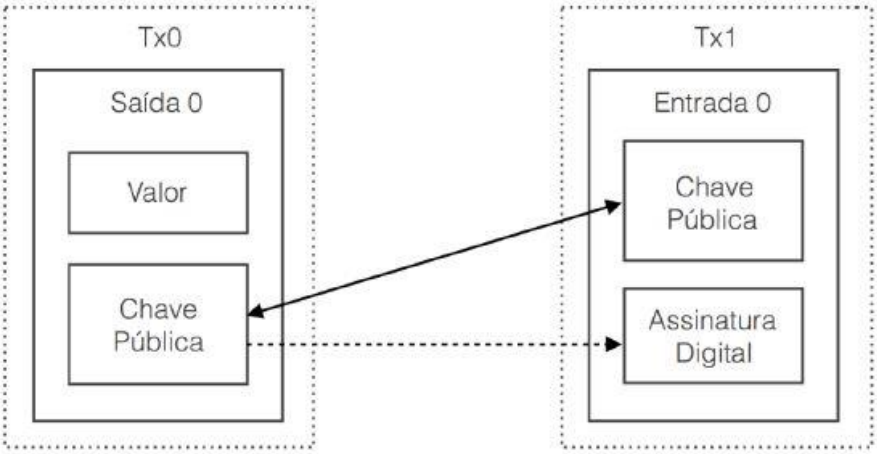
Fonte: PIRES 2016 p. 29

A assinatura digital através de uma chave privada é usada para criptografar a mensagem, ou seja, é utilizada para assinar uma mensagem, e também através da chave pública é feita a verificação da assinatura. Assim ao inserir uma chave pública na saída de uma transação, somente aquele que tem a chave privada correspondente é autorizado a fazer uso daquela saída.

> “No processo de validação da transação, a chave pública informada no campo Entrada é comparada com a chave pública previamente inserida na saída. Caso elas sejam diferentes, a transação é considerada inválida e não é propagada para os demais nós da rede.” (PIRES, 2016 p. 29)

Se por algum motivo ocorrer igualdade de chaves, a verificação ocorre com a chave pública que foi informada e confirmada primeiro. Caso a assinatura seja autêntica, em palavras mais técnicas se a decriptação com o uso da chave pública fazer a revelação dos dados da transação, então a validação da transação é confirmada e a informação repassada para os demais nós da rede e a coleta em bloco de mineração é realizada. Caso a chave não seja validada, o processo é descartado. Na figura seguinte vemos como ocorre o processo de validação de registros com chaves públicas e privadas.

Figura 9: Processo de validação do registro.

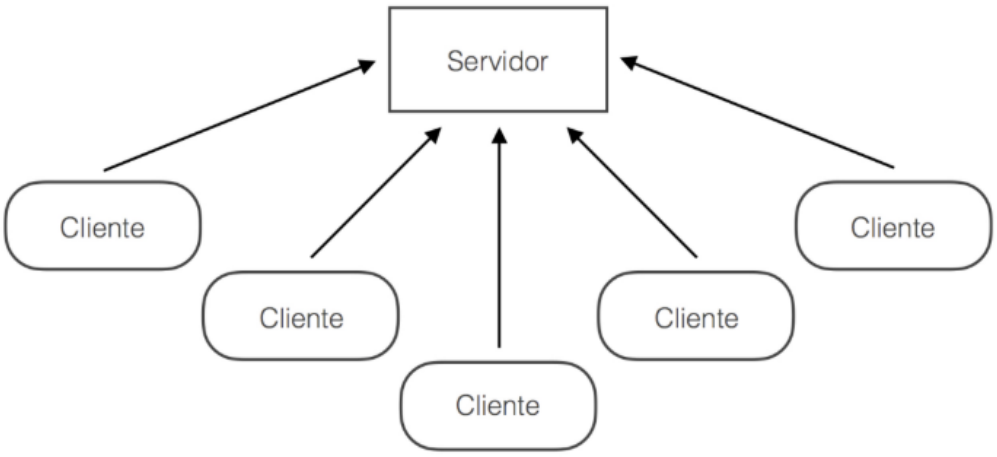


Fonte: PIRES 2016 p. 30

3.3 Redes p2p (peer-to-peer)

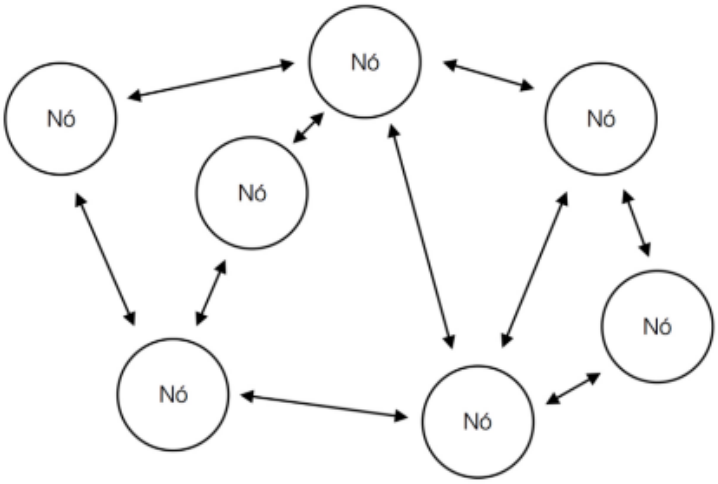
Utilizando uma arquitetura descentralizada em que as maquinas são chamadas de nó, executam funções de cliente e servidor ao mesmo tempo, diferenciando-se da arquitetura cliente-servidor que apesar de parecidas, se diferenciam pela cliente-servidor enviar solicitações ao servidor e precisar aguardar sua resposta. As figuras a seguir demonstram as estruturas dos dois modelos de arquitetura.

Figura 10: Arquitetura Cliente-servidor



Fonte: Wang, 2009, *adaptado*

Figura 11: Arquitetura P2P



Fonte: Wang, 2009*, adaptado*

No modelo cliente-servidor o desempenho do servidor é deteriorado à medida que o número de requisições dos clientes aumenta. Em redes p2p, o desempenho geral da rede aumenta à medida que cresce o número de nós da rede. (PIRES, 2016 p. 24)

> "Normalmente, cada nó da rede pode realizar upload e download ao mesmo tempo e novos nós podem entrar na rede enquanto outros nós estão saindo, caracterizando um modelo de alta flexibilidade e ainda transparente ao usuário final. Uma característica interessante de redes p2p é capacidade de tolerância a erros." (PIRES, 2016 p. 24)

> "Quando um nó é desconectado da rede, a aplicação p2p pode continuar a operar utilizando outros nós que permanecem ativos. Na arquitetura cliente-servidor a conexão é interrompida se um servidor é desligado. Outra característica importante das redes p2p, especialmente para a utilização com o blockchain, é o seu caráter descentralizado. Informações transmitidas por um nó da rede, podem rapidamente serem replicadas para máquinas em diversos lugares do mundo, tornando praticamente impossível apagar ou alterar registros espalhados em um número tão grande de nós." (PIRES, 2016 p. 24)

3.4 Mineração ou validação de blocos

Após a validação a transação está apta para ser coletada por um bloco e seguir para o processo mineração, um nó minerador é responsável por coletar os registros que deseja inserir na Blockchain no meio de todas os registros que foram validados, logo após é realizado o cálculo da raiz da árvore de Merkle e depois passaa executar o algoritmo *proof of work,* em tradução literal, prova de trabalho.

A prova de trabalho consiste num desafio criptográfico que é utilizado para confirmar e garantir que o nó realizou o trabalho a ele atribuído, o Bitcoin por sua vez

utiliza uma prova de trabalho baseada em outro modelo denominado de Adam Back. As outras aplicações da Blockchain manuseiam outras variações deste modelo, desde que atendam aos dois princípios principais que são:

a) Confirmar e garantir que o nó realizou a quantidade de trabalho a ele atribuído.
b) Garantir que a prova entregue é objetivamente verificável.

Caracteristicamente uma prova de trabalho consiste num processo probabilístico e a como em todo processo desse tipo a probabilidade de sucesso depende da dificuldade que foi estabelecida.

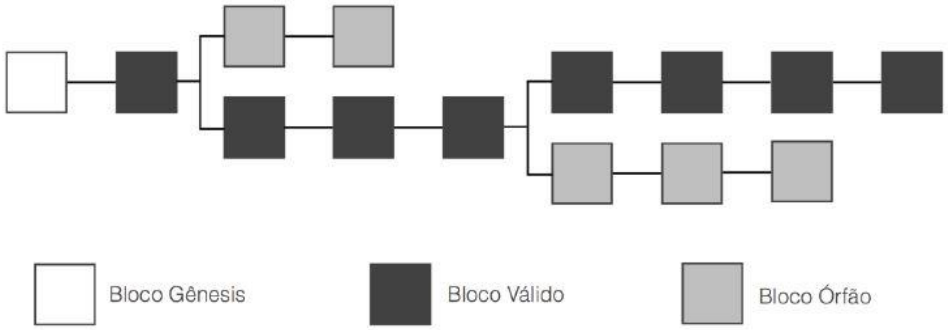
> "No bitcoin, por exemplo, a prova de trabalho é encontrar um valor chamado *nonce* cujo duplo hash SHA256 desse valor com a raiz de Merkle seja igual ou menor que um parâmetro T. A busca por esse valor é feita por tentativa e erro. Quanto menor o parâmetro T, menor a probabilidade de sucesso e mais difícil é conseguir realizar a prova de trabalho. Quanto maior o parâmetro T, maior a probabilidade e mais fácil encontrar um *nonce* válido. O protocolo do bitcoin ajusta o parâmetro T automaticamente a cada 2016 blocos para garantir que as provas de trabalho e, consequentemente, a mineração de um bloco aconteça, em média, a cada 10 minutos." (PIRES, 2016 p. 30)

Ao ser validado, o bloco é instantaneamente publicado na rede p2p (ponto-aponto) para que todos os outros nós tenham conhecimento do feito. Cada um dos nós recebe um bloco novo e faz a verificação para sabe se realmente é um bloco ainda não recebido, todo bloco tem uma numeração chamada de altura do bloco que é uma numeração incremental, após a verificação o blockchain recebe uma cópia do bloco e replica aos nós adjacentes. Este processo é repetido por toda a rede com a finalidade de haver uma conformidade entre os nós da rede no que diz respeito ao estado da cadeia dos blocos.

> "Caso aconteça de dois nós realizarem a prova de trabalho com uma diferença de tempo pequena, eles vão propagar blocos de mesma altura na rede gerando o que é chamado de Corrida de Blocos. O protocolo resolve essa questão da seguinte maneira: o maior segmento da cadeia de blocos é o segmento válido, isto é chamado de Regra da Maior Cadeia - *Longest Chain Rule*. Dessa forma, cada nó adiciona blocos recém-criados à cadeia de maior altura até que uma bifurcação da cadeia se torne maior e a outra sequência de blocos seja abandonada, gerando os chamados blocos órfãos. No fim, existe apenas uma cadeia que liga o último bloco validado de volta até o primeiro bloco da cadeia. No caso do blockchain do bitcoin, este primeiro bloco é chamado de bloco gênesis." (PIRES, 2016 p. 31)

A figura abaixo mostra a Regra da Maior Cadeia:

Figura 12: Rede de Maior Cadeia



Fonte: (PIRES, 2016 p. 31)

3.5 Ataque 51%

"51% é o ataque em que um ou mais nós da rede alcançam capacidade de processamento total igual ou superior a 51% da capacidade de processamento de toda a rede." (PIRES, 2016 p. 33)

"Os nós sempre estendem a corrente mais longa. Para um ataque cibernético, seria necessário que uma maioria (51%) de nós mineradores entrasse em conluio. Isso envolveria um custo computacional altíssimo." [Nakamoto 2008].

"Deste modo, seria possível que transações feitas a partir de endereços não autorizados ou transações utilizando um valor já utilizado por outra transação (*dual spending*) fossem validadas pelos nós mal-intencionados." (PIRES, 2016 p. 33)

> "Como o atacante possui mais da metade da capacidade de processamento da rede, a bifurcação da cadeia (também chamado de *fork*) com os registros fraudados cresceria de maneira mais rápida que a bifurcação autêntica, validando transações que deveriam ser descartadas. Isto é chamado de ataque 51%." (PIRES, 2016 p. 33)

Algumas considerações importantes a respeito deste tipo de ataque:

- Não existem registros de ataques que obtiveram sucesso desde a criação da ferramenta em 2009.

- "Caso um minerador possuísse 51% ou mais da capacidade de mineração da rede, seria mais vantajoso minerar as transações e receber as recompensas do protocolo do que efetuar um ataque à rede." [Nakamoto, 2008]

- A possibilidade de se alcançar 51% da capacidade de processamento total da rede do blockchain do bitcoin é muito pequena.

- "Outras tecnologias de blockchain, implementadas após o bitcoin, como o Litecoin, realizam um a prova de trabalho mais 'democrática' de modo que a simples capacidade de processamento não representa uma grande vantagem sobre os outros mineradores." [Torres, 2013];

- “Há propostas em alguns lugares do mundo, como no Reino Unido, para a regularização do processo de mineração de modo a impedir a existência de um minerador com tamanha capacidade de processamento.” [UK Gov, 2015]

> “Enfim, embora faça algum sentido do ponto de vista teórico, o ataque 51% não é uma ameaça na prática. Acredita-se que o maior risco relacionado ao ataque esteja na perda de confiança na tecnologia devido a existência de um super minerador e a consequente desvalorização da aplicação.” (PIRES, 2016 p. 33)

4. CONSIDERAÇÕES FINAIS

O mundo está em constante evolução, o homem está em constante evolução, as tecnologias talvez sejam a que vemos evoluir de forma mais rápida. A evolução tecnológica nos presenteou com uma de suas melhores obras através do desconhecido que usa o codinome Satoshi Nakamoto, o Bitcoin e o Blockchain que tem atraído olhares no decorrer dos últimos anos.

Sob a luz das ideias apresentadas por outros autores aprendemos acerca da tecnologia que se estudada e aplicada de forma, coerente e responsável irá ajudar milhões espalhados pelo mundo, irá diminuir gastos e tornar processos difíceis e burocráticos em processos mais rápidos e simples.

O bitcoin destacou-se pelo fato de ter as suas transações sendo feitas de forma rápida e segura e com custo baixo e mais importante, é uma moeda livre, não pertence a um banco ou a um governo, a liberdade e sua valorização têm atraído bastante adeptos espalhados pelo mundo.

Ulrich (2014, p. 17) afirma que “a invenção do Bitcoin é revolucionária e resolve o problema do gasto-duplo sem que haja a necessidade de um terceiro.” O blockchain faz isso distribuindo o registro a todos os usuários através de uma rede *peer-to-peer,* na tradução literal, ponto-a-ponto.

A ferramenta Blockchain nos mostrou que tem um enorme potencial de ser aplicada para organizações permitindo transações seguras sem que ocorra a necessidade de um agente intermediador e existe uma grande expectativa girando em torno da ferramenta no que diz respeito aos impactos que ela pode produzir na sociedade dos próximos anos, porém vimos que ainda temos muito a aprender e o que conhecemos é como uma gota no oceano do que ainda precisa ser descoberto e aprimorado para que a sociedade se beneficie da tecnologia.

Diante do apresentado podemos confiar num sistema que elimina o intermediador para a realização de transações e que a ferramenta é segura e garante a integridade e disponibilidade das informações ali armazenadas.

4.1 Trabalhos futuros

Alguns trabalhos futuros podem ser desenvolvidos sob a luz deste trabalho que está sob uma luz maior de outros livros e autores.

Um estudo mais aprofundado pode analisar o impacto social do Bitcoin em sociedades menos desenvolvidas, assim como também pode ser estudado o uso da ferramenta Blockchain em categorias diferentes do Bitcoin.

O bitcoin e a ferramenta Blockchain são as bases deste trabalho e os seus rumos para estudos são os mais variados possíveis. Ressaltamos a importância e a relevância da ferramenta para a sociedade que só tem a ganhar com a nova tecnologia que está revolucionando o mercado.

REFERENCIAS

ARAÚJO, Henrique Pereira de; SILVA, Rebecca Bignardi Arambasic Rebelo da. A TECNOLOGIA DIGITAL BLOCKCHAIN: ANÁLISE EVOLUTIVA E PRAGMÁTICA. Revista FATEC Zona Sul, São Paulo, Junho 2017.

BLOCKCHAIN Demo. [S. l.], 2019. Disponível em: https://anders.com/blockchain/hash.html. Acesso em: 1 jul. 2019.

FRANCO, P. Understanding Bitcoin: Cryptography, engineering and economics. John Wiley & Sons, 2014.

GREVE, Fabiola et al. Blockchain e a revolução do consenso sob Demanda. Simpósio Brasileiro de Redes de Computadores, Campos do Jordão, São Paulo, 2018. Disponível em: http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/Capitulo5.pdf. Acesso em: 3 jul. 2019.

LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum. In: IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP, 9, 29-30 de setembro, Campinas, São Paulo, 2016. Disponível em: <http://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf>. Acesso em: 4 abr. 2019

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Eletronic Cash System. 2008. 9 p. Disponivel em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: jun. 2019.

NARAYANAN, Arvind et al. Bitcoin and cryptocurrency technologies: a Comprehensive Introduction. Princeton: Princeton University Press, 2016. 336 p.

PIRES, Timoteo Pimenta. Tecnologia Blockchain e suas Aplicações para Provimento de Transparência em Transações Eletrônicas. Distrito Federal, 2016. Xiii, 56p., 210 x 297mm (ENE/FT/UnB, Bacharel, Engenharia de Redes de Comunicação, 2016).

SWAN, Melanie. Blockchain: Blueprint for a New Economy. Sebastopol, California: O'Reilly MediaInc., 2015.149 p.

TORRES, Osman X. J. (2013) —Tecnologias de suporte ao conceito de criptomoeda‖. Universidade Federal de Pernambuco. Centro de Informática. Recife, 2013. p. 13.

UK Gov; HM Treasury - UK Government. (2015) "Digital currencies: response to the call for information‖. ISBN 978-1-910337-91-2.

ULRICH, Fernando. Bitcoin - A moeda na era virtual. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.